U.S. DEPARTMENT OF ENERGY | OFFICE OF ELECTRICITY

Communications in the Electric Grid: An Evolving Interdependent Ecosystem between the Grid and Communications Utilities

Our Nation's electric system is transitioning from a centralized, producer-controlled network to a distributed, consumer-interactive model that is often referred to as a smart grid. A fully functioning smart grid will feature ubiquitous sensors throughout the transmission and distribution grid while continuing to balance electric supply (generation) with consumer demand (load). These sensors will need to collect and share data with consistent and well-defined latency, higher bandwidth, and two-way communications to transport information between utilities and consumers through distributed or cloud-based computing as needed to make the data actionable. Secure communications are critical for the successful operation of this modern electric grid.

Secure Communications

A secure communications system protects the end-to-end physical pathway that transports data from origin to destination. That pathway may: involve different transmission methods, such as optical fiber, copper wire, and microwave; transport diverse data including grid state information and control messaging; and use a variety of analog and digital formats. Securing this end-to-end communications pathway—which is essential for reliable grid operations—involves preventing unauthorized access and monitoring traffic to identify anomalous activity without compromising the confidentiality, integrity, or availability of the data. Communications security methods complement cybersecurity approaches used to protect data at origin and destination.

This white paper will briefly discuss several factors driving the continued electric grid evolution and the communication requirements. These factors include:

1. Evolution of hardware, software, and communications used in the electric grid over the last several decades at unprecedented scales,
2. Rapid adoption of variable, renewable distributed energy resources (DERs) and intelligent loads in the electric grid, and
3. An increased threat landscape due to more intense weather patterns and external actors.

To achieve a safe, reliable, and secure electrical system, the supporting secure communications networks must evolve, as well. Are there opportunities for collaboration between energy sector stakeholders (utilities, regulators, service providers, and consumers) and the telecommunications sector (vendors, standards bodies, and service providers) to explore secure communications concerns and develop potential solutions? This white paper offers some open-ended questions to drive further discussion. A series of follow-on white papers will explore some of these factors in more detail.

How is electric grid operational technology changing, and what are the implications for the electric industry's secure communications requirements?

The electric grid was originally designed to support one-way power flow from a small number of large, centralized generation plants to customers. Electric grid operators controlled how much power could be produced at any given moment, instantaneously matching generation to customer load. In most utilities,

the customer load followed predictable patterns, allowing grid operators to develop predictable controls and mechanisms to match generation with load. This allowed the electric grid to be monitored and controlled with limited communications, predominantly with analog communication systems that were, in many cases, one-way. Over the last several decades, the communication requirements for monitoring and controlling the electric grid have changed dramatically. The growth of distributed intelligence, coupled with broadband communications and automated control systems, has driven the need for greater communication bandwidth and reliability.[1]

As illustrated in Table 1, since the late 20th century, the electric grid has undergone transition to hardware capable of digital measurement, sensing, local intelligence, and distributed control capabilities. Hundreds of millions of additional devices with digital capabilities (including communications) have been added to the electric grid infrastructure across the Nation. Additionally, new software has been implemented to interact with this hardware (energy management systems, outage management systems, DER management systems, etc.) to effectively monitor, coordinate, and control the electric grid. Electric utilities expanded their deployment of two-way digital communication networks to connect these new hardware and software solutions. The reliability, speed (from microseconds to days), and geographic distribution drove communications requirements for this hardware and software. Will propriety communication systems be adaptable to the evolving requirements of the smart grid?

Table 1: Grid Evolution, from 2020 Smart Grid Systems Report[2]

Grid Component	Status in 20th Century	21st Century – Smart Grid Developments Underway
Grid Hardware *Examples: Relays, reclosers, circuit breaker*	Well-developed by early 20th century. Almost all devices and equipment remained electromechanical until 1990s.	Controls moving to digital capabilities for measurement, sensing, local intelligence, and distributed control.
Grid Communications/Networks *Examples: Field area networks, wide area networks*	Use of various limited, one-way analog communications technologies (e.g., frame relay circuits) joined in later century with satellite, cellular, unlicensed radio.	Communications reaching out to customer premises. Two-way digital communications for wide area networks and field area networks.
Grid Software *Examples: GIS, OMS, DMS, EMS*	Limited centralized software for major applications (e.g., security-constrained economic dispatch).	Distributed software pervasive in field devices and systems, Centralized software capabilities greatly increased.

How is the increasing penetration of DERs and variable bulk generation affecting the electric industry's secure communications requirements?

There has been a dramatic increase in variable renewable generation deployment and DER participants, including individual consumers and technology service providers (e.g., aggregators). This increase is being driven by technological advancements, cost reductions in technologies, and state policy and regulatory action related to climate change and dependence on fossil fuels. Renewables, primarily driven by variable generation sources such as wind and solar, are expected to be the largest source of

[1] United States Department of Energy, "Grid 2030" A National Vision for Electricity's Second 100 Years, July 2003. https://www.energy.gov/oe/articles/grid-2030-national-vision-electricitys-second-100-years

[2] United States Department of Energy, Smart Grid System Report, January 2022. https://www.energy.gov/sites/default/files/2022-05/2020%20Smart%20Grid%20System%20Report_0.pdf

generation by 2030; simultaneously, there has a been a steady growth of installed DER capacity closer to the edge of the system.

These resources move the electric grid away from a relatively small number of centralized spinning generation sources to a large number of DER technologies. Many of these DER technologies, which DER participants—rather than the electric utility—own and control, are introducing significant complexity and uncertainty to electric grid planners and operators. Many of these generation sources, like wind and solar generation, are not as predictable as spinning-based generation sources due to weather and environmental variability. DER participants add volatility; for example, a DER generator can become a load within a few hours.

Consumer-owned DER assets will likely connect to the electric utility via various communications broadband options that are out of the electric utility's control. The need for near real-time monitoring, coordination, and control of these DER assets will be critical to grid operations and stability due to the unpredictability of the net generation from these DER assets. The increasing dependency of electric grid operations on the telecommunication infrastructure has led to a fundamental shift in how the electric utility perceives communication and communication security. What are the challenges for obtaining secure, reliable information from highly disparate sources? What are the opportunities for the electric and communications sectors to collaborate on the solution?

The controllability of DER assets is fundamentally different from that of centralized generation due to the former's geographically dispersed nature. As reported in the October 2022 Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid,[3] "These DER installations will be managed in a different manner from traditional power operations due to their dispersed nature, resulting in a heavy reliance on communications for remote control and monitoring (and very likely the internet)." Are the current standards for interoperability and communications connectivity for these technologies moving in the right direction or rapidly enough? How will DERs integrate with an electric utility's existing control network and how do we secure the communications? Where do cybersecurity and secure communications systems intersect, and what role does secure communications play in operational security?

To what degree is the evolving grid increasing the threat from bad actors and the susceptibility to the impacts of natural disasters, and how can secure communications mitigate these threats?

Both the communications and electric sectors are considered critical infrastructure vital to the operation of the Nation's economy. Human actors continue to try to exploit vulnerabilities within these systems for political or financial purposes while increasingly intense and frequent weather patterns are causing more physical damage.

[3] United States Department of Energy, Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid, October 2022. https://www.energy.gov/sites/default/files/2022-10/Cybersecurity%20Considerations%20for%20Distributed%20Energy%20Resources%20on%20the%20U.S.%20Electric%20Grid.pdf

As the threat envelope continues to increase, the electrical system and its supporting communication infrastructure become natural targets. What protections are being deployed for the underlying communication infrastructure while considerable efforts continue in the private and public sector to develop new cybersecurity methods to protect control data?

The increasing need for communications across disparate networks (different operators, telecommunications providers, etc.) increases reliance on infrastructure outside the grid operators' control, increasing the potential threat envelope for disruption. How do grid operators (e.g., utilities and coordinators) ensure reliability and agility in the grid as it evolves with growing information needs and increased communications sector interdependence?

The impacts of climate change and more frequent natural disasters are also driving the need for greater reliability and agility in grid management, which requires more frequent status information and additional data from grid-connected assets. Increasing disruptions due to natural disasters have made the interdependence of the electric utilities and communications companies more apparent. Agility in grid control relies on communications technology, yet these technologies rely on electric power, as does commercial communication infrastructure that carries the information.[4] How do changes in the grid landscape and more frequent disruptions from climate impacts affect both sectors? What are the opportunities for collaboration and the sharing of insights and approaches to manage these emerging challenges? What insights could be gained from enhanced collaboration?

Conclusion

This white paper describes the evolving nature of the electric grid and the communication challenges associated with evolving hardware and software requirements, rapid adoption of DERs, and increased threats. The goal of this white paper is to initiate discussions on collaboration between energy sector stakeholders (utilities, regulators, service providers, standards bodies, vendors, and consumers) and the communications sector (vendors, standards bodies, and service providers) to explore secure communications concerns and develop potential solutions. The long-term goal is to engage an active set of stakeholders to collaborate on areas of concern, emerging requirements, and new capabilities related to secure communications systems for a reliable electric system of the 21st century. We welcome you to join us at our upcoming sessions at the 2023 UTC Telecom & Technology Conference and other venues throughout 2023 and 2024.

[4] O'Reilly, G.P.; Richman, S.H.; Kelic, A. "Power, telecommunications, and emergency services in a converged network world" 2007 6th International Workshop on Design and Reliable Communication Networks, 2007, pp. 1–6. 10.1109/DRCN.2007.4762253